REMARKS

This application has been carefully reviewed in light of the Office Action dated November 7, 2001. Claims 1 to 14, 18 to 20 and 22 remain in the application, and with Claims 15 to 17 and 21 having been cancelled. Claims 1, 10, 14, 18, 20 and 22, the independent claims herein, have been amended. Reconsideration and further examination are respectfully requested.

As a formal matter, Applicant notes that the Office Action did not include either a Form PTO-948 (Notice Of Draftsperson's Patent Drawing Review) or an indication by the Examiner that the drawings have been reviewed and are acceptable. In the absence of an indication otherwise, Applicant presumes the drawings are acceptable, but respectfully requests clarification of this matter in the next communication.

Turning to the substance of the Office Action, Claims 1 to 3, 10 to 12 and 14 were rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 5,535,277 (Shibata), Claims 18, 19 and 20 to 22 were rejected under § 102(b) as allegedly being anticipated by U.S. Patent No. 5,253,293 (Shigemitsu), and Claims 4 to 9, 13 and 15 to 17 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 5,398,283 (Virga) in view of Official Notice. Reconsideration and withdrawal of the rejections are respectfully requested.

The present invention concerns encryption of digital information. Conventionally, digital information is encrypted utilizing an encryption key that is resident on a computer workstation or one that is obtained over a network and stored resident on a computer workstation. Because the encryption key remains, resident on the computer

workstation, a hacker can readily obtain the encryption key and utilize it to decrypt the encrypted digital information. Of course, a user can erase the encryption key at a later time, but the time lag between encrypting the information and erasing key is generally sufficient for a hacker to still be able to obtain the encryption key.

The present invention addresses the foregoing by erasing the encryption key rather than allowing the key to remain resident on the computer. According to the invention, digital information is encrypted with an encryption key, and coincident with completion of the encryption process, the encryption key is erased. In an alternative arrangement, the encryption key may itself be encrypted by a second encryption key, with both encryption keys then being erased coincident with completion of the second encryption process. As a result, the time lag between the encryption process and erasing of the encryption key is significantly reduced and the likelihood of a hacker being able to obtain the encryption key is reduced.

Referring specifically to the claims, amended independent Claim 1 is an image input apparatus comprising conversion means for converting an image signal into digital information, encryption means for encrypting the digital information by using an encryption key, and erasing means for erasing the encryption key coincident with completion of the digital information being encrypted by the encryption means.

Amended independent Claims 10 and 14 are method and computer program claims, respectively, that substantially correspond to Claim 1.

Amended independent Claim 18 is an image input apparatus comprising conversion means for converting an image signal into digital information, information

encryption means for encrypting the digital information by using an internal encryption key disposed within the image input apparatus, means for inputting from an external source an external encryption key for encrypting the internal encryption key, key encryption means for encrypting the internal encryption key by using the external encryption key, and erasing means for erasing both the internal encryption key and the external encryption key coincident with completion of encrypting the external encryption key by the key encryption means.

Amended independent Claims 20 and 22 are method and computer program claims, respectively, that substantially correspond to Claim 18.

The applied art, alone or in combination, is not seen to disclose or to suggest the features of Claims 1, 10, 14, 18, 20 and 22. More particularly, the applied art is not seen to disclose or to suggest at least the feature of erasing an encryption key coincident with completion of digital information being encrypted (Claims 1, 10 and 14), or erasing both an internal encryption key and an external encryption key coincident with completion of encrypting the external encryption key with the external encryption key (Claims 18, 20 and 22).

Shibata is seen to disclose that an encryption/decryption circuit 403 encrypts data using an encryption key maintained by the circuit. After encryption is completed, the encrypted data is transmitted over a phone line. In Shibata, a user can register (i.e., create), change and delete an encryption key by assigning a ten-digit number. The user performs these processes via an operation section 7. (See column 4, lines 48 to 51 and column 7, lines 39 to 45.) However, the encryption key used to encrypt the data in Shibata is

maintained in the device and is not erased coincident with the encryption process being completed. Rather, the key is only erased by user action, which may be performed some time after the key is used at least once to encrypt data or before the key is ever used. Therefore, Shibata is not seen to disclose or to suggest at least the feature of erasing an encryption key coincident with completion of digital information being encrypted (Claims 1, 10 and 14), or erasing both an internal encryption key and an external encryption key coincident with completion of encrypting the external encryption key with the external encryption key (Claims 18, 20 and 22).

Shigemitsu is seen to disclose that a random number D is generated and used to cipher data and that the random number is then ciphered by a secret key code T_s to form a cipered code $T_s(D)$. The ciphered code $T_s(D)$ is then ciphered by a public key code R_s. Thus, Shigemitsu merely teaches encrypting data with a first (internal) key and encrypting the first key with a second (external) key. However, Shigemitsu is not seen to disclose or to suggest at least the feature of erasing an encryption key coincident with completion of digital information being encrypted (Claims 1, 10 and 14), or erasing both an internal encryption key and an external encryption key coincident with completion of encrypting the external encryption key with the external encryption key (Claims 18, 20 and 22).

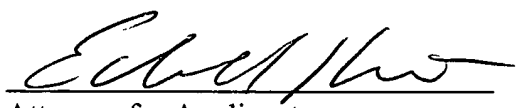
Virga is seen to disclose a card-key being used for inputting an encryption key, which may comprise inputting an encryption key from an external source. However, Virga is not seen to disclose or to suggest at least the feature of erasing an encryption key coincident with completion of digital information being encrypted (Claims 1, 10 and 14),

or erasing both an internal encryption key and an external encryption key coincident with completion of encrypting the external encryption key with the external encryption key (Claims 18, 20 and 22).

In view of the foregoing, all of independent Claims 1, 10, 14, 18, 20 and 22 are believed to be allowable over the applied art. Accordingly, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicant

Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200
CA_MAIN 40117 v 1

APPENDIX

VERSION WITH MARKINGS TO SHOW CHANGES MADE TO CLAIMS

1. (Amended) An image input apparatus comprising:

conversion means for converting an image signal into digital information;

encryption means for encrypting the digital information by using an encryption key; and

erasing means for erasing said encryption key [after] coincident with completion of the digital information [has been] being encrypted by the encryption means.

10. (Amended) An image input method comprising the steps of:

converting an image signal into digital information;

encrypting the digital information by using an encryption key; and

erasing said encryption key [after] coincident with completion of the digital information [has been] being encrypted in the encrypting step.

14. (Amended) An encryption processing program stored in a computer-readable medium, comprising:

a step of converting an image signal into digital information;

a step of encrypting the digital information by using an encryption key; and

a step of erasing said encryption key [after] coincident with completion of the digital information [has been] being encrypted in the encrypting step.

15. to 17. (Canceled)

18. (Amended) An image input apparatus comprising:

conversion means for converting an image signal into digital information;

information encryption means for encrypting the digital information by using an internal encryption key disposed within said image input apparatus;

means for inputting from an external source an external encryption key for encrypting said internal encryption key; [and]

key encryption means for encrypting said internal encryption key by using said external encryption key; and

erasing means for erasing both the internal encryption key and the external encryption key coincident with completion of encrypting the external encryption key by the key encryption means.

20. (Amended) An image input method comprising the steps of:

converting an image signal into digital information;

encrypting the digital information by using an internal encryption key disposed

within said image input apparatus;

obtaining from an external source an external encryption key for encrypting said internal encryption key; [and]

encrypting said internal encryption key by using said external encryption key; and

erasing both the internal encryption key and the external encryption key coincident with completion of the step of encrypting the internal encryption key using the external encryption key.

21. (Cancelled)

22. (Amended) An encryption processing program stored in a computer-readable medium, comprising:

a step of converting an image signal into digital information;

a step of encrypting the digital information by using an internal encryption key disposed within [said] an image input apparatus;

a step of obtaining from an external source an external encryption key for encrypting said internal encryption key; [and]

a step of encrypting said internal encryption key by using said external encryption key; and

a step of erasing both the internal encryption key and the external encryption key

coincident with completion of the step of encrypting the internal encryption key.

CA_MAIN 40118 v 1